BEST AVAILABLE IMAGES

Defective images within this document are accurate representation of The original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

Proceedings of ICSP' 96

Key Distribution System For Digital Video Signal

Xiao-wen Yang , Zhi-hang Zheng
Ph.D. student , Professor
Video Communication Lab , Dept. Electronic Engineering
Shanghai Jiaotong University,Shanghai, P.R.China
Tel : 86-21-62825456-53
Fax : 86-21-62820892

Abstract: Today although traditional analogue video signal has served the information broadcasting network effectively , its drawbacks make its usage limited . So it comes the digital video signal using modern compress technics , and the quality of the digital programmes is improved . Once extra programmes such as feature films became available , their providers need to be paid , and conditional access system have to be found of financing these programmes. Compressed digital video signal needs new scramble methods and key distribution system for conditional access, copyright protection and finance. This paper suggests some digital scramble tools and the design of an efficient and realistic key distribution system for the digital video information broadcasting and any other environment which the MPEG-2 bit stream be employed. The scrambling methods and the key distribution system in this paper are based on the format of the transport stream packet of MPEG-2 transport layer.

Standard television formats such as PAL, NTSC and SECAM transmitted through terrestrial transmitters using amplitudes modulation have been used primarily for entertainment broadcasting for more than 47 years, and cannot fulfill all of today's requirements. There is a growing need for digital video, which includes moving pictures and associated sound for various applications such as digital storage media, television broadcasting and communication. In this case, digital motion video can be manipulated as a form of computer data and can be stored on various storage media, transmitted and received over existing and future networks and distributed on existing and future broadcasting channels. But in this digital environment, where perfect copying of a video program is easy, everyone in the distribution network footprint can receive the same program,except for a few transmission errors. Owners of information resources are fearful of releasing proprietary information to an environment which appears to be lacking in security. It means that every receiver in this network can get the program, and that might not be what the broadcasters and program owners wanted. As we know that the installation and operation of any program distribution system,as well as the production and copyright protection of the programmes will depend on the availability of finance. They may be operating a private network or a digital pay-TV system. So there comes subscription-television or pay-TV, a major component of the audiovisual landscape. They need to protect their transmitted signal, so that he can collect revenue for its sale, or to ensure its privacy. Conditional access, for pay-TV as well as for other professional purposes, makes the programmes which may consist of a combination of video, audio, data and teletext, to be transmitted to the special subscribers, not to anyone else. The viewer has access to programmes only when certain conditions have been satisfied. Although the most usual condition will be that money has to be paid, this is by no means the only possible arrangement.

0-7803-2912-0

Scrambling Introduction

Because each user accesses the same signal in any broadcasting environment, the program components (sound and picture, sometimes completed by various data) should be broadcasted in a scrambled form. Such scrambling should be sufficiently robust to deter any attack by an intruder breaking the code of the components. To do this, the program must be obscured by an encoder, using some process that can be reversed by legitimated decoders, so that the programmes can be protected from "pirates" , a term which refers generally to any party who attempts to access the programmes through surreptitious means

Fig.1 shows a general scheme of a secure channel. A program message, M, also called plaintext, is encrypted by an invertible transformation, F_{K_1}, that produces a ciphertext $S = F_{K_1}(M)$. The ciphertext is transmitted over a public over air channel, and therefore can be received by everyone. An authorized receiver decodes the program by the transformation $G_{K_2}(S) = F_{K_1}^{-1}$.

$$G_{K_2}(S) = F_{K_1}^{-1}\left[F_{K_1}(M)\right] = M$$

The parameter K_1 and K_2, called the encryption key and the decryption key respectively, specify the used scrambling and descrambling transformation $F_{K_1}(\bullet)$ and $G_{K_2}(\bullet)$. So in the decoder end, if the program message be decrypted, it is necessary to get the decryption key K_2. In public key system, $K_1 \neq K_2$, and the transformation F_{K_1} is a one-way function.

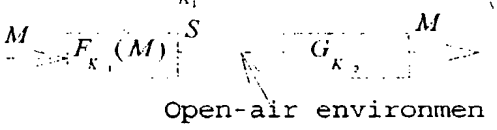

Fig.1 General secure transmissi scheme

In any worthwhile secure information delivery system, the security cannot be ultimately based on maintaining the security of any fixed part of the system--the signal format, the scrambling method, the encryption processes and the fixed key. If the security is to be based on any secret information, then that information must be kept secret. But some of the design information cannot be kept secret at all. So it is worthwhile to increase the security of the entire system by very often changing the scrambling key . If the fixed key is used in digital TV broadcasting, it is possible to try a known plaintext attack. By subscribing to a pay-TV program, it is easy to know both the plaintext and the corresponding ciphertext. Such attacks are very efficient in breaking coding based on PRBS built by linear shift registers. As we know, the video scrambling method itself is not the basis of the security, it can be widely advertised. But the rapidly changing pattern of the scrambling is where the security resides. Therefore , the key management in conditional access system is very important.

Scrambling Compressed Video Signal

The Moving Pictures Expert Group of the ISO and the CCITT has recently proposed a generic compression algorithm for digital TV signal, the MPEG-2 algorithm, to be standardized worldwide. In this specifications, known as ISO/IEC 13818-2, there are three kinds of picture:1.) I-frames, 2.) P-frames 3.) B-frames .

The decoding process can start only when an I-frame is received, mostly at the beginning of the macroblock of the slice in an I-frame. So an I-frame is sent every 10 frames. The synchronization of the decryption has to be compatible with such an approach in order to deliver descrambled pictures with limited delays. Each frames information is transmitted by the discrete cosine transform (DCT) and finally the DCT coefficients are adaptively coded by a 2-D Huffman coded. The coded data stream should be multiplexed into the fixed-length transport stream. In such a digital TV conditional access system, the scrambling method needs to operate on the three basic data structures of MPEG-2:

- Transport Stream Packets
- PES Packets

· Sections

The main application is the scrambling of MPEG-2 Transport Stream Packets . Each packet consists of 188 bytes and is constructed in accordance with the MPEG-2 transport syntax and semantics. Many scrambling methods are applied to the payload , Fig.2 and Fig 3 are two examples.

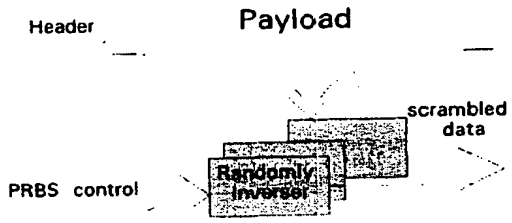

Fig 2 Randomly inverse the payload

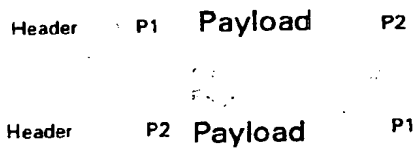

Fig 3 Intercange the payload

In Fig.2 every bit or byte located in the payload is inverted randomly. In Fig.3 , each payload is cut into two parts , each of the two parts is then interchanged effectively rotated about the cut point, the cut points as well as which bit should be inverted in Fig.2. are determined as part of the encryption mechanism by a pseudo-random-binary sequence generator. The initial state of the PRBS' shift register should be transmitted to the appropriate receivers, which is needed to recover the original digital video information.

Key Distribution For Digital Video

Because the main function of a conditional access system is the secure transmission of the control word to the appropriate receivers, a layered key structure must be employed. The issuer key (IK), the main function of which are : loading the lower level keys (programmer distribution key, service key), and invalidating lower level keys. The programmer distribution key (PDK) used to encipher the parameters to be stored in the security processor (services keys, entitlements ···). This key is generally distributed to the users by the program provider. The service key (SK) used to encipher the control words. These keys (IK, PDK, SK) should be enciphered and transmitted to users. A realistic keys distribution block diagram is shown in Fig.4.

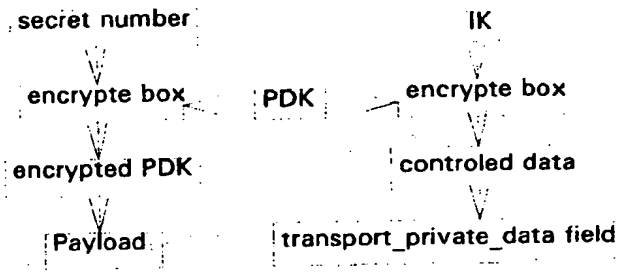

Fig 4 key distribution system for digital video stream

How these keys be transmitted in the MPEG-2 bit stream ?

According to the specification ISO/IEC 13818, there are 2-bits flag in the transport Link Header after 13-bit PID, which is called transport_scrambling_control. Digital video conditional access system makes use of this flag to denote whether the video data stream is scrambled. From a practical point of view, multi-layered key management system is related to every decoder's production number, and the basic key is mapped with that number. The basic key can be embedded in the microprocessor of the decoder, or a detachable smart card. At the encoder end, the payload of the MPEG-2 bit transport packet will be scrambled by the PRBS which is controlled by the service key. After being enciphered by the programmer distribution key , the service key will transmitted in the adaptive field of the stream packet and change frequently , when the splicing_point_data_flag and the transport_private_data_flag are set , the enciphered issuer key can be transmitted in the transport_private_data field .

With the help of the transport_scrambling_control field in the Link Header , the programmer distribution

key is determined in the cryptograms book of the decoder . When the field was set by 00 , and the PID field was assigned to key transmission control , the encoder will start to transmit the new ciphered programmer key encrypted by the secret series number to the entitled user's decoder in the field after the Link Header of the transport layer , at the same time , the adaptation field control should be set to 01 , to indicate no adaptive field be transmitted . In the user entitlement inquiry system of the CA (Conditional Access) control center it is determined by the user's payment that which secret number to be used to encrypt the programmer key , so that the control center can control the appropriate decoder

After receives the input scrambled data at the receiving end , firstly the decoder will judge according the flags in the Link Header if there is new programmer distribution key be transmitted . If yes , it will decrypt the new programmer distribution key by the entitled user secret number, and put the decrypted new programmer distribution key to the appointed location in the microprocessor of the receiver . The decoder which has no entitlement cannot decrypt the new programmer distribution key . If no , the decoder will use the old programmer distribution key appointed by the transport scrambling_control field to decrypt the encrypted data in the transport_private_data to get the service key , and then descramble the payload located after the adaptation header to recover the compressed video data . The recovered compressed video data will put into the MPEG-2 decoder to be de-compressed , at last the plain video , audio and other data will be displayed at the user terminate.

Conclusion

This key management system can be used not only in the digital TV system like digital terrestrial or cable broadcasting environment , but also in the multimedia environment which the information broadcasting should be paid . But we should know that the standardization of a universal solution for key management of the conditional access system is unrealistic , due to the political problems arising from secrecy .

References

[1] Michon, Vicent "Single conditional access system for satellite-cable and terrestrial TV", IEEE Trans. on consumer Electronics v35 n 3 Aug.1989. p 464-468

[2] Tsubakiyama Hidek, Koga Keiichiro, "Security for information data broadcasting with conditional-access control ", IEEE Global Telecommunications Conference v 1 1993, publ by IEEE Service Center, Piscataway, NJ,USA,93CH3250-8,p 164-170

[3] Bagenal.P.W, Upton.S.W, "Customer management and the eurocrypher conditional access system at British Satellite Broadcasting", IEE Conference Publication n 327,Publ by IEE. Michael FAraday House, Stevenage, English. p 270-277

[4] Louis Claude Guillou , Jean luc Giachetti, "Encipherment and Conditional Access". SMPTE Journal v 103, n 6, Jane 1994.